CLAIMS

1. A method of performing a reduction operation in a cryptographic calculation, the method comprising selecting a modulus having a first section with a plurality of "1" Most Significant Word states and a second section which comprises a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and operating (S1-S5; S10-S12; S20-S26) a reduction operation on the modulus/multiple.

2. A method according to Claim 1 comprising effecting a plurality of multiplication operations (S1).

3. A method according to Claim 2 comprising effecting a plurality of multiplication operations followed by effecting a reduction operation (S1, S2).

4. A method according to Claim 3 comprising repeating the combined multiplication operations and reduction operation (S1, S2).

5. A method according to any preceding claim comprising using a multiple of the modulus/multiple.

6. A method according to any preceding claim wherein, when the last multiplication gives an overflow (S4), the overflow is added to a part of the selected number.

7. A method according to Claim 6 wherein, when the overflow addition step (S4) produces an overflow, then n_0' (S5) is added to the overflow.

8. A method according to any preceding claim, wherein the carry c between two adjacent multiplications is effected as the addend in the next multiplication (S2).

9. A method according to any preceding claim comprising monitoring the number of leading "1"s to determine if the number is less than (k-2).

10. A method according to Claim 6 comprising initiating the next calculation when the number of leading "1"s is less than (k-2).

11. A method according to any preceding claim the method comprising operating 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits.

12. A method according to any of Claims 1 to 10 the method comprises operating 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

13. A method according to any of Claims 1 to 10 the method comprising operating 256-bit ECC and a word size of 64-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.

14. A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of any one or more of Claims 1 to 13 when said product is run on a computer.

15. A computer program directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of any one or more of Claims 1 to 13 when said program is run on a computer.

16. A carrier, which may comprise electronic signals, for a computer program of Claim 15.

17. Electronic distribution of a computer program product of Claim 14 or a computer program of Claim 15 or a carrier of Claim 16.

18. Apparatus for performing a reduction operation in a cryptographic calculation, the apparatus comprising means to select a modulus or a multiple of a modulus having a first section with a plurality of "1" states and a second section having a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and means (10-17) for operating a reduction operation on the modulus/multiple.

19. Apparatus according to Claim 18 comprising means (10-17) to effect a plurality of multiplication operations.

20. Apparatus according to Claim 19 comprising means (10-17) to effect a plurality of multiplication operations followed by a reduction operation.

21. Apparatus according to Claim 20 comprising means (10-17) to repeat the combined multiplication operations and reduction operation.

22. Apparatus according to any of Claims 18 to 21 comprising means (10-17) to use a multiple of the modulus/multiple.

23. Apparatus according to any of Claims 18 to 22 comprising means (10-17), when the last multiplication gives an overflow, to add the overflow to a part of the selected number.

24. Apparatus according to Claim 23 comprising means (10-17), when the overflow addition step produces an overflow, to add n_0' to the overflow.

25. Apparatus according to any of Claims 18 to 24 (10-17) comprising means to effect the carry c between two adjacent multiplications as the addend in the next multiplication.

26. Apparatus according to any of Claims 18 to 25 (10-17) comprising means to monitor the number of leading "1"s to determine if the number is less than (k-2).

27. Apparatus according to any of Claims 18 to 26 comprising means (10-17) to initiate the next calculation when the number of leading "1"s is less than (K-2).

28. Apparatus according to any of Claims 18 to 27 with means (10-17) for 192-bit EEC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

29. Apparatus according to any of Claims 18 to 27 with means (10-17) for 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

30. Apparatus according to any of Claims 18 to 27 with means (10-17) for 256-bit ECC and a word size of 64-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.

31. A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of Figures 1 to 5 of the accompanying drawings.

32. Apparatus for performing a reduction operation in a cryptographic calculation, the apparatus substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of Figures 1 to 5 of the accompanying drawings.

33. A method of performing a reduction operation in a cryptographic calculation, the method substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of Figures 1 to 5 of the accompanying drawings.